UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Jamia Wright (DOB: 08/23/2001)	)	Case No. 24-910M(NJ)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin *(identify the person or describe the property to be searched and give its location)*:

See Attachment A3.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B1.

YOU ARE COMMANDED to execute this warrant on or before September 23, 2024 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ❒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Nancy Joseph, United States Magistrate Judge.

(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____.

Date and time issued: 9/16/2024 @ 3:47 p.m.

Judge's signature

City and state: Milwaukee, Wisconsin

Nancy Joseph, United States Magistrate Judge

Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A3

The location to be searched is the person and effects of Jamia WRIGHT (DOB: 08/23/2001).

ATTACHMENT B1
Items To Be Seized

All records and information relating to violations of 18 U.S.C. §§ 1512(a)(2)(A), 1512(a)(2)(B), 1512(b)(1), and 1512(k), including but not limited to:

1. Indicia of occupancy, residency or ownership of the premises and things described in the warrant, including but not limited to utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease or rental agreements, addressed envelopes, escrow documents and keys.

2. Cellular telephones, computers, iPads, tablets, flash drives, or other electronic devices and all electronic storage areas on the device including text messages, Facebook messages, audio and digital video recordings.

3. Any records and information regarding correspondence, notations, logs, receipts, journals, books, records and other documents regarding violations of 18 U.S.C. §§ 1512(a)(2)(A), 1512(a)(2)(B), 1512(b)(1), and 1512(k), and identifying additional co-conspirators and any payment for proceeds from violations of 18 U.S.C. §§ 1512(a)(2)(A), 1512(a)(2)(B), 1512(b)(1), and 1512(k).

4. Records and information relating to witness tampering and a conspiracy to do the same.

5. Records and information relating to the identity or location of the suspects and any co-conspirators, the purpose and scope of the conspiracy, and any overt acts in furtherance thereof.

For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as

well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as

microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Jamia Wright (DOB: 08/23/2001)

Case No.24-910M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A3.

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B1.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 1512(a)(2)(A), 1512(a)(2)(B), 1512(b)(1), and 1512(k).	Witness tampering, and conspiracy to do the same

The application is based on these facts:

See the attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Jacob Dettmering, Special Agent (FBI)

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 9/16/2024

Judge's signature

City and state: Milwaukee, Wisconsin

Nancy Joseph, United States Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, Jacob A. Dettmering, being first duly sworn, hereby depose and state as follows:

I. BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since January 7, 2018. I was assigned to the FBI Capital Area Gang Task Force (CAGTF) in Baton Rouge, Louisiana from June 15, 2018, to April 1, 2020. Since April 1, 2020, I have been assigned as the Task Force Coordinator for the Milwaukee Area Safe Streets Task Force (MASSTF). Since 2018, I have investigated violations of federal law, directed drug and street gang investigations, obtained and executed search and arrest warrants related to the distribution of illegal narcotics, and debriefed confidential informants and cooperating defendants. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), in that I am empowered by law to conduct investigations of and to make arrests for federal offenses.

2. I have been trained in a variety of investigative and legal matters, including the topics of Fourth Amendment searches, the drafting of search warrant affidavits, and probable cause. I have participated in criminal investigations, surveillance, search warrants, interviews, and debriefs of arrested subjects. As a result of this training and investigative experience, I have learned how and why violent actors typically conduct various aspects of their criminal activities.

3. This affidavit is based upon my personal knowledge and upon information reported to me by other federal and local law enforcement officers during the course of their official duties, all of whom I believe to be truthful and reliable.

4. Throughout this affidavit, reference will be made to case agents. Case agents are those federal, state, and local law enforcement officers who have directly participated in this investigation, and with whom your affiant has had regular contact regarding this investigation.

5. Because this affidavit is submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only facts that I believe are sufficient to establish probable cause.

6. For the reasons discussed herein, there is probable cause to believe that violations of 18 U.S.C. §§ 1512(a)(2)(A), 1512(a)(2)(B), 1512(b)(1), and 1512(k), have been committed by Kaira PRINCE (dob: 10/19/1998) and Jamia WRIGHT (dob 08/23/2001). There is also probable cause to believe that in the premises located at **5310 W Hustis St, Unit B, Milwaukee, WI,** more fully described in Attachment A1; **on the person of Kaira PRINCE (dob: 10/19/1998)**; and **on the person of Jamia WRIGHT (dob 08/23/2001)** are items that constitute evidence of witness tampering and conspiracy to commit witness tampering in violation of Title 18, United States Code, Sections 1512(a)(2)(A), 1512(a)(2)(B), 1512(b)(1), and 1512(k).

7. I further make this affidavit in support of applications for search warrants under Federal Rule of Criminal Procedure 41 and 18 U.S.C. §§ 2703(c)(1)(A) for information about the location of the cellular telephone assigned call number **262-951-8586 ("Target Cell Phone #1")**, whose service provider is Verizon ("Service Provider") a wireless telephone service provider headquartered at 1095 Avenue of the Americas, New York, NY 10036; and for information about the location of the cellular telephone assigned call number **414-248-8142 ("Target Cell Phone #2)**, whose service provider is T-Mobile ("Service Provider") a wireless telephone service provider headquartered at 4 Sylvan Way, Parsippany, NJ 07054. **Target Cell Phone #1** is described herein and in Attachment A4, and the location information to be seized is described herein and in Attachment B2. Target Cell Phone #2 is described herein and in Attachment A5, and the location information to be seized is described herein and in Attachment B3.

8. Because the warrant applications for **Target Cell Phone #1** and **Target Cell Phone #2** seek the prospective collection of information, including cell-site location information, that may fall within the statutory definitions of information collected by a "pen register" and/or "trap and trace device," see 18 U.S.C. § 3127(3) & (4), I also make this affidavit in support of an application by the United States of America for orders pursuant to 18 U.S.C §§ 3122 and 3123, authorizing the installation and use of pen registers and trap and trace devices ("pen-trap devices") to record, decode, and/or capture dialing, routing, addressing, and signaling information associated with each communication to or from **Target Cell Phone #1** and **Target Cell Phone #2**.

9. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1512(a)(2)(A), 1512(a)(2)(B), 1512(b)(1), and 1512(k), have been committed and may continue to be committed by Kaira PRINCE (dob: 10/19/1998) and Jamia WRIGHT (dob 08/23/2001). There is also probable cause to believe that the location information described in Attachment B2 and Attachment B3 will constitute evidence of these criminal violations and will lead to the identification of individuals who are engaged in the commission of these offenses.

10. The court has jurisdiction to issue the proposed warrant because it is a "court of competent jurisdiction" as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, see 18 U.S.C. § 2711(3)(A)(i).

II. PROBABLE CAUSE

11. The United States, including the Federal Bureau of Investigation, is conducting a criminal investigation of PRINCE and WRIGHT regarding violations of 18 U.S.C. §§ 1512(a)(2)(A), 1512(a)(2)(B), 1512(b)(1), and 1512(k).

12. The "Wild 100s," also known as the "Shark Gang" or "SNG," is a violent street gang in Milwaukee, that engaged in various criminal activities, including crimes of violence, illegal firearms possession, drug distribution, conspiracy, and fraud, in Milwaukee and elsewhere.

13. On April 25, 2023, a Grand Jury in the Eastern District of Wisconsin returned a sealed 43-count indictment charging 30 members and affiliates of the Wild

100s with mail fraud conspiracy, in violation of 18 U.S.C. § 1349; mail fraud, in violation of 18 U.S.C. § 1341; murder-for-hire, in violation of 18 U.S.C. § 1958; use and discharge of a firearm during a crime of violence resulting in death, in violation of 18 U.S.C. § 924(c), 924(j); a conspiracy to violate the laws of the United States, in violation of 18 U.S.C. § 371, and various firearms and drug possession crimes, in Case No. 23-CR-077. That case was recently set for trial, and the trial is scheduled to begin in November 2024.

14. On Wednesday, September 11, 2024, lead defendant Ronnell Bowman, who is charged with murder-for-hire, along with other crimes, called one of the Government's witnesses (CW-1) on a recorded jail call, and referenced his upcoming trial. Bowman indicated that CW-1 would be testifying against him, and that Bowman would soon receive the witness list. Bowman also referenced CW-1's alleged ongoing relationship with another of the Government's witnesses (CW-2). During the call, Bowman suggests that he could provide CW-1 "3gs," a possible reference to $3,000, and suggests that CW-1 has to "clear my motherfuckin name." Bowman claims that CW-1 and others are "lying on" him, are the reason that he was charged, and tells CW-1 to call "dude," which appears to be a reference to CW-2 and inquire about why "he's lying on me, bro." Bowman tells CW-1 to tell CW-2 to "clear my name."

15. On Friday, September 13, 2024, at approximately 8:55 p.m., CW-2 observed a Facebook post by Facebook username "Micheal Turner" that listed three addresses in Milwaukee, Wisconsin. The first address posted by "Michael Turner" is the current residence of CW-2's mother and sister, and CW-2's prior residence in Milwaukee. CW-2

provided a screenshot of this Facebook post to investigators, along with screenshots of text messages that he received.

16. At approximately 8:12 p.m. on Friday, September 13, 2024, CW-2 received the following messages from call number 414-264-9704:

We on yo ass nigga them addresses got dropped hide ya family snitch ass nigga

Scary ass nigga you still in Texas we fina show you some

[The first of the three addresses posted by Facebook username "Micheal Turner" and current residence of CW-2's mother and sister.]

17. At approximately 8:57 p.m. on Friday, September 13, 2024, CW-2 received the following message from call number 414-376-5411:

1-2 we coming for you 3-4 tell yo momma lock them doors 5-6 you shouldn't have snitched 7-8 that was your biggest mistake 9-10 she better let me in[.]

18. Case agents ran both phone numbers through a law enforcement telephone application to identify a service provider. The search indicated that xx9704 has a provider of "Sinch-Onvoy Spectrum-NRS-10X/2". The xx5411 number had a listed provider of Sinch Voice-NSR-10X-Port/1. Based on that information, case agents know that the numbers utilized are considered Voice over Internet Protocol "VOIP." Case agents know through training and experience that VOIP's are often used when individuals are committing crimes, in an attempt to conceal the actual device they used to commit the crime and conceal their identity as well.

19. Your affiant also reviewed the Facebook page for "Micheal Turner" and

found that in the "About" section, the account has it listed as a female, current resident of the City of Milwaukee, and an MATC Milwaukee graduate from 1982. The URL for the page is https://facebook.com/diane.stacy.167, and there is a picture in the publicly viewable account which has a cake which reads, "Happy Birthday Diane." There is also a picture which is from June 1, 2015, and shows a Milwaukee County Sheriff's Deputy escorting a black male through what appears to be a courthouse. The caption for the photo is, "Number 1grandson Tyvon". Additionally, There was a picture posted on March 20, 2015, with the caption, "Happy Birthday Tyvon today you turn ? Years old."

20. I am also aware that in November of 2023 an unredacted copy of an interrogation video of CW-2, during which CW-2 provided information to members of the Milwaukee Police Department about various crimes committed by the Wild 100s was obtained and posted by Vernell Hamilton, and posted to social media by Vernell Hamilton, another Wild 100s member and co-defendant in 23-CR-77. The interrogation video of CW-2 had been produced as discovery in a homicide prosecution in Milwaukee County Circuit Court, and based upon Vernell Hamilton's posting of the video and screenshots of various documents, it appears that Hamilton had obtained the entire set of discovery in the state homicide case.

21. Your affiant submitted a request to Sinch for any and all information pertaining to xx9704 and xx5411. Sinch followed up, stating xx9704 belonged to an application called Pinger, Inc and xx5411 belonged to TextNow, Inc.

22. Your affiant sent a request to Pinger, Inc and TextNow Inc. for information

related to the respective phone numbers. Only TextNow, Inc. responded to the request. TextNow responded with a spreadsheet with numerous IP addresses related to text messages during the time period for the text message sent by xx5411. The IP address that covered the timeframe for the text message was identified as 65.29.226.78.

23. Your affiant ran the IP address 65.29.226.78 through the American Registry for Internet Numbers (ARIN) and found that the owner of that IP address was Charter Communications. Your affiant sent a request to Charter Communications for three separated IP number hits with specific port numbers. Charter Communications replied and provided the subscriber for that IP address was Kaira PRINCE, dob: October 19, 1998, with a physical device address of **5310 W Hustis St, #B, Milwaukee, WI**. The phone number they had listed for Prince was 414-803-2242.

24. Your affiant sent a request to Meta Inc. (Facebook) for subscriber information and IP address logins for the account username "Micheal Turner". Meta returned the subscriber information, which was Micheal Turner and the last three IP address which the account used to login which was 2603:6000:aa00:4f97:1968:4707:8d45:975d. They also provided a GPS location for the login which plotted to **5310 W Hustis St, Milwaukee, WI.**

25. 22. Your affiant ran the IP address 2603:6000:aa00:4f97:1968:4707:8d45:975d through the American Registry for Internet Numbers (ARIN) and found that the owner of that IP address was Charter Communications. Your affiant sent a request to Charter Communications for three

separated IP number hits with specific port numbers. Charter Communications replied and provided the subscriber for that IP address was Kaira Prince, Date of Birth October 19, 1998, social security account number 387-83-2685, with a physical device address of 5310 W Hustis St, #B, Milwaukee, WI. The phone number they had listed for Prince was 414-803-2242.

26. Your affiant ran Kaira PRINCE through the Wisconsin Court System website and found Milwaukee County Case Number 2023PA000468PJ. This specific court case was a paternity case involving Kaira S. PRINCE and Jaquan Allante Wright. Your affiant knows that Jaquan Wright was indicted on April 25, 2023 (see 23-CR-77) with 29 other Wild 100s gang members, including Ronnell Bowman.

27. Your affiant found a publicly viewable Instagram page for PRINCE, "Kairaiveryy." The pages profile picture is of Jaquan Wright and the text below it reads, "Jaquan Wife" with a heart emoji. The pictures, which are publicly viewable, show PRINCE and two children, one of which is known to be the child of Prince and Wright.

28. Your affiant knows that in Ronnell Bowman was charged with five (5) separate counts, including murder for hire in violation of Title 18, United States Code, Sections 1958(a) and 2(a) in *United States v. Ronnell Bowman, et al*, 23-CR-77. On August 22, 2024, Judge Stadtmueller set trial dates in 23-CR-77 for November of 2024.

29. Case agents listened to recorded jail calls made from the Ozaukee County Jail , where Ronnell Bowman and Jaquan Wright are currently detained. Thus far, case agents have identified at least three calls made that are related to this investigation.

30. First, on September 12, 2024, a call was placed to **414-248-8142 (Target Phone #2)**, a phone number which lists to Jamia WRIGHT in the Ozaukee County jail call database. The database further describes Jamia WRIGHT as Jaquan Wright's sibling. This call was placed using a different inmate's personal identification number (PIN), i.e., not Ronnell Bowman's PIN; however, your affiant recognized the calling party's voice as Ronnell Bowman's, based upon my familiarity with Bowman's voice given my experience in this investigation. In the call, WRIGHT claims to have received a call from CW-1 after CW-1 spoke to Bowman as described above. WRIGHT seems to claim that she has a recording of either CW-1 or CW-2 demanding money from her and threatening that she needs to pay by Friday or Jaquan Wright will be sentenced to life. Your affiant is aware that Jaquan Wright had his sentencing hearing and was sentenced in Case Number 23-CR-77 on Friday, September 13, 2024. In that same call, Ronnie Bowman tells Jamia WRIGHT "I need to make them not credible" and "[CW-1] already not credible… I need to make [CW-2] not credible." Bowman encourages Jamia WRIGHT to speak with his private investigator saying "that will really really help me."

31. Second, case agents located and listened to a second call, made from the Ozaukee County Jail, made to **262-951-8586 (Target Phone #1)** at approximately 3:12 p.m. on Friday, September 13, 2024. This call was placed using a different inmate's personal identification number (PIN), i.e., not Ronnell Bowman's PIN; however, your affiant recognized the calling party's voice as Ronnell Bowman's, based upon my familiarity with Bowman's voice given my experience in this investigation. This phone number **262-**

951-8586 (Target Phone #1) lists in the Ozaukee County Jail system as belonging to Kaira PRINCE, and notes that she is a "girlfriend" of Jaquan Wright. In this call, your affiant again recognizes the male caller's voice as Ronnell Bowman's. The call also begins with him saying "This Ronnie Bow man!" and asking if he is speaking to Kaira or "Chop"?. Based upon case agents' review of a large number of related calls made during this time frame, your affiant is aware that "Chop" is the nickname of Jamia WRIGHT. Both Kaira PRINCE and Jamia WRIGHT, aka "Chop" respond that they are on the line. During this call, Bowman, Jamia WRIGHT and Kaira PRINCE then discuss recent contacts the women claim to have had with CW-1 and CW-2.

32. Your affiant is aware that during this second call Bowman also asks questions about Jaquan Wright's sentencing which had just occurred that afternoon. Both women respond with their observations about the Judge and the "DA" in a manner which indicates both were present in Court that afternoon, and therefore likely in the State and Eastern District of Wisconsin that evening when the threatening text messages were sent.

33. Third, case agents located and listened to a recorded jail call made using Jaquan Wright's PIN to 262-951-8586 (Target Cell Phone #2) that took place at approximately 8:40 p.m., or less than an hour after CW-2 received the first threatening text message, and before CS-2 received the second threatening text message at 8:57 p.m. In this call, Jaquan Wright asks the female, believed to be PRINCE, why she is laughing. The woman replies that she and "Jamia" (i.e., WRIGHT) were "fucking with [CW-2]" and "just fucking with him" and "scaring his ass" with a "text-now number" "acting like we

gonna pull up on him." Based upon my training, experience, and the investigation to date, your affiant believes that "gonna pull up on him" means going to shoot him or kill him.

34. On September 14, 2024, your affiant obtained a tracking warrant, signed by the Honorable Magistrate Judge Nancy Joseph in the Eastern District of Wisconsin (24-905M(NJ)), for the Facebook account "Micheal Turner." On September 15, 2024, the GPS location data for the "Michael Turner" revealed that its location plotted to **5310 W Hustis St, Milwaukee, WI**.

TECHNICAL BACKGROUND

35. In my training and experience, I have learned that the Service Providers are companies that provide cellular communications service to the general public. I also know that providers of cellular communications service have technical capabilities that allow them to collect and generate information about the locations of the cellular devices to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular device and, in some cases, the "sector" (i.e., faces of the towers) to which the device connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device.

Accordingly, cell-site data provides an approximate general location of the cellular device.

Cell-Site Data

36. Based on my training and experience, I know that the Service Providers can collect cell-site data on a prospective basis about Target Cell Phones #1 and #2. Based on my training and experience, I know that for each communication a cellular device makes, its wireless service provider can typically determine: (1) the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower to which the customer was connected at the end of the communication; and (5) the duration of the communication. I also know that wireless providers such as the Service Providers typically collect and retain cell-site data pertaining to cellular devices to which they provide service in their normal course of business in order to use this information for various business-related purposes.

37. Based on my training and experience, I know that Verizon also can collect per-call measurement data, which Verizon also refers to as the "real-time tool" ("RTT"). RTT data estimates the approximate distance of the cellular device from a cellular tower based upon the speed with which signals travel between the device and the tower. This information can be used to estimate an approximate location range that is more precise than typical cell-site data.

E-911 Phase II / GPS Location Data

38. I know that some providers of cellular telephone service have technical capabilities that allow them to collect and generate E-911 Phase II data, also known as GPS data or latitude-longitude data. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device's signal using data from several of the provider's cell towers. As discussed above, cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data is typically less precise that E-911 Phase II data. Based on my training and experience, I know that the Service Providers can collect E-911 Phase II data about the location of , Target Cell Phones #1 and #2 including by initiating a signal to determine the location of Target Cell Phones #1 and #2 on the Service Provider's network or with such other reference points as may be reasonably available.

Pen-Trap Data

39. Based on my training and experience, I know each cellular device has one or more unique identifiers embedded inside it. Depending on the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number ("ESN"), a Mobile Electronic

Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), a Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), an International Mobile Subscriber Identifier ("IMSI"), or an International Mobile Equipment Identity ("IMEI"). The unique identifiers – as transmitted from a cellular device to a cellular antenna or tower – can be recorded by pen-trap devices and indicate the identity of the cellular device making the communication without revealing the communication's content.

Subscriber Information

40. Based on my training and experience, I know that wireless providers such as the Service Providers typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless communication service. I also know that wireless providers such as the Service Provider typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular device and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify the Target Cell Phone's user or users and may assist in the identification of co-conspirators and/or victims.

41. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

42. As described above and in Attachments B1, this application seeks permission to search for records that might be found on the premises or on the persons listed in Attachments B1, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

43. *Probable cause.* I submit that if a computer or storage medium is found on the premises or on the persons listed in Attachments A1, A2, and A3, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

44. *Forensic evidence.* As further described in Attachment B1, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the premises and on the persons listed in Attachments A1, A2, and A3 because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data

typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses an electronic device to threaten another, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit

a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

45. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises or persons for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

46. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

a. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the

storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

b. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

47. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for in Attachments A1, A2, and A3 and B1 would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

48. Because several people share may share the premises located at 5310 West Hustis Street, Unit B, Milwaukee, Wisconsin as a residence, it is possible that the premises will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

AUTHORIZATION REQUEST

49. Based on the foregoing, I request that the Court issue the proposed warrants for Target Cell Phones #1 and #2, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41, referenced in Attachment A4 and A5.

50. I further request that the Court direct the Service Providers to disclose to the government any information described in Section I of Attachment B2 and Attachment B3 that is within its possession, custody, or control.

51. I also request that the Court direct the Service Providers to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B2 and Attachment B3 unobtrusively and with a minimum of interference with the Service Provider's services, including by initiating a signal to determine the location of Target Cell Phones #1 and #2 on the Service Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall reasonably compensate the Service Providers for reasonable expenses incurred in furnishing such facilities or assistance.

52. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 30 days after the collection authorized by the warrant has been completed. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing

immediate notice to the subscriber or user of Target Cell Phones #1 and #2 would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). As further specified in Attachment B2 and Attachment B3, which is incorporated into the warrants referenced in Attachments A4 and A5, the proposed search warrants referenced in Attachments A4 and A5 do not authorize the seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

53. Because the warrant will be served on the Service Providers, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the Target Cell Phones #1 and #2 outside of daytime hours.

54. Additionally, based upon the information set forth above , there is probable cause to believe that violations of 18 U.S.C. §§ 1512(a)(2)(A), 1512(a)(2)(B), 1512(b)(1), and 1512(k), have been committed by Kaira PRINCE (dob: 10/19/1998) and Jamia WRIGHT (dob 08/23/2001) and that in the premises located at **5310 W Hustis St, Unit B, Milwaukee, WI,** more fully described in Attachment A1; **on the person of Kaira PRINCE**

(dob: 10/19/1998), as described in Attachment A2; and **on the person of Jamia WRIGHT (dob 08/23/2001),** as described in Attachment A3; are items that constitute evidence of witness tampering and conspiracy to commit witness tampering in violation of Title 18, United States Code, Sections 1512(a)(2)(A), 1512(a)(2)(B), 1512(b)(1), and 1512(k).

55. I submit that this affidavit supports probable cause for a warrant to search the premises and persons described in Attachments A1, A2, and A3 and seize the items described in Attachment B1.

ATTACHMENT A3

The location to be searched is the person and effects of Jamia WRIGHT (DOB: 08/23/2001).

ATTACHMENT B1
Items To Be Seized

All records and information relating to violations of 18 U.S.C. §§ 1512(a)(2)(A), 1512(a)(2)(B), 1512(b)(1), and 1512(k), including but not limited to:

1. Indicia of occupancy, residency or ownership of the premises and things described in the warrant, including but not limited to utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease or rental agreements, addressed envelopes, escrow documents and keys.

2. Cellular telephones, computers, iPads, tablets, flash drives, or other electronic devices and all electronic storage areas on the device including text messages, Facebook messages, audio and digital video recordings.

3. Any records and information regarding correspondence, notations, logs, receipts, journals, books, records and other documents regarding violations of 18 U.S.C. §§ 1512(a)(2)(A), 1512(a)(2)(B), 1512(b)(1), and 1512(k), and identifying additional co-conspirators and any payment for proceeds from violations of 18 U.S.C. §§ 1512(a)(2)(A), 1512(a)(2)(B), 1512(b)(1), and 1512(k).

4. Records and information relating to witness tampering and a conspiracy to do the same.

5. Records and information relating to the identity or location of the suspects and any co-conspirators, the purpose and scope of the conspiracy, and any overt acts in furtherance thereof.

For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as

well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as

microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.